OPTIONAL FORM NO. 10

UNITED STATES GOVERNMENT

Memorandum

U-0425/SC-2

TO : DR

DATE: 20 August 1974

FROM : SC-2

SUBJECT: Security Leaks - Legal Tools and Precedents

1. The attached Legal Brief covers the following subject:

Legal Authorities for Protection of Security Information; Punitive Actions Applying to Breach of Security.

2. The Preface to the attached brief is in effect my conclusions drawn from this brief. Appendixes to the study are verbatum copies of pertinent statutes.

3. The Columbia Law Review article of May 1973 entitled The Espionage Statutes, contained an appropriate summation of a writer's task in reviewing the statutory coverage of this area of the law:

> "When we turned to the United States Code to find out what Congress had done, we became absorbed in the effort to comprehend what the current espionage statutes mandate with respect to the communications and publication of defense information. The longer we looked, the less we saw. Either advancing myopia had taken its toll, or the statutes implacably resist the effort to understand. In any event, whether the mote be in our eye or in the eyes of the draftsmen, we have not found it possible to deal with the espionage statutes except at forbidding length."

STAT

Very respectfully,

[redacted]

General Counsel, DIA

1 Enclosure a/s

DIA review Completed.

Encl 2

Sanitized Copy Approved for Release 2010/04/20 : CIA-RDP94B00280R001200130005-7

LEGAL BRIEF

Legal Authorities for Protection of Security Information; Punitive Actions Applying to Breach of Security

Preface

I. Background

Recent Cases

II. Authority for Classifying Material

III. Important Elements to be Considered in Espionage Statutes

IV. a. Espionage Statutes

b. Cases in Support of Espionage Statutes

V. Other Important Provisions of Title 18 (Criminal Code)

VI. Miscellaneous Applicable Punitive Statutory Provisions

VII. Protection of Defense Information by Other Democratic Nations

a. British Official Secrets Acts

b. Canada (Official Secrets Acts)

c. France (French Penal Code)

VIII. Appendix - Copies of Pertinent Statutes

Tab A - Title 18 US Criminal Code Espionage Laws

B - Title 42 Atomic Energy Act

C - Miscellaneous Applicable Statutes

D - The Official Secrets Act (England)

E - French Penal Code

PREFACE

The following Conclusions can be drawn from the attached study of the Espionage Statutes and other pertinent criminal provisions.

The Espionage Statutes and other miscellaneous provisions are in my opinion more significant as enforcement tools than would be indicated by the limited number of incidents in which they have been used.

It is to be noted that the Government argued the Pentagon papers case without regard to using the Espionage Statutes as authority but relying on the inherent powers of the President as Commander-in-Chief. The Supreme Court did not seize upon this as an opportunity to proclaim any wide guidance in this area by court-made law. The Court in fact was reluctant to act affirmatively without statutory guidance and rendered a very narrow opinion.

The relevant provisions for use in enforcement of security violations are found in 18 USC 793 to 798 (Criminal Code) and certain other Miscellaneous statutory provisions. The overriding question of interpretation of these statutes is whether newspapers, their reporters, their informants or anyone who investigates or retains

defense information as a prelude to public speech or disclosure is covered by these statutes. In most instances, people who make efforts to obtain defense related information, whether journalists or spies, do so because they envision the possibility of communicating it to others.

Title 18 USC 794 pertains only to defense information communicated with the intended or predictable consequences that the revelation will be used to injure the United States or to the advantage of any foreign nation or with the intent that the information shall be communicated to the enemy.

Title 18 USC 798 applies only to certain classified information relating to communications.

Title 18 USC 793 (a) and (b) are more properly to be applied in situations of unauthorized acquisition of information. They do not prohibit communication of any kind. Both sections, however, cover actions which in many incidents occur prior to publication.

Subsections 793(c), (d), and (e) are sweeping statutory authorities and make criminal, receipt of material knowing it to be obtained in violation of other espionage provisions. These provisions do not explicitly on their face require ulterior intent to harm the United States. It is my opinion that in appropriate cases courts could, in future actions,

interpret these particular sections as making criminal nearly all unauthorized acquisitions by newspapers of "National Defense" information. This term has been broadly defined.

Much has been written concerning the meaning in the Espionage Statutes of the words "related to the national defense," as being Constitutionally vague. The defendents in the case of Gorin v. United States claimed because of their innocuous character, the reports, the subject of the case, Naval Intelligence Reports, could not relate to national defense. The Supreme Court approved the trial court instructions to the jury that "national defense includes all matters directly and reasonably connected with the defense of our nation against its enemies."

The US constitutional system severely limits the criminal law enforcement power of the United States Government, requiring more exact definition of Federal crime, than for instance, that required under the British Official Secrets Act.

The British Official Secrets Act would seem to prohibit almost all types of communication of official secrets to or between unauthorized persons. The United States laws are much more limited on this problem. None

of the United States statutes go as far as section 2 of the Official Secrets Act in restricting persons unconnected with the government from disclosing classified information they have received. The present criminal statutes in my opinion provide many legal tools for protecting the country from unauthorized disclosure of potentially damaging information. The area of greatest weakness in existing statutes for control of security violations is in the area of "prior restraints," the term given for prohibition of publication of items which are held without proper authority. The denial of injunction in the proceedings in the "Pentagon Papers" case is a prime example. The Supreme Court Justices in this case referred, time and again, to the reluctance of Congress to enact what might appear to be "censorship" provisions. It is true that in reviewing the legislative history of the "espionage statutes" Congress exhibited reluctance to enact any statutes that bordered on censorship of the press. An example is 18 USC 793, 1(b):

> "Nothing in this act shall be construed to authorize, require, or establish military or civilian censorship***."

In the "Pentagon Papers" case Justice White stated he would have no difficulty in sustaining convictions under the espionage provisions of Title 18 provided that it would not involve imposition of "prior restraints," i.e., prohibition of publication of unauthorized items held.

He further stated:

> "It is clear that Congress has addressed itself to the problem of protecting the security of the country and the national defense from unauthorized disclosure of potentially damaging information. It has not, however, authorized the injunction remedy against threatened publication.
>
> The issue of guilt or innocence would be determined by procedures and standards quite different from that purported to govern the injunctive proceedings."
>
> * * * *
>
> "To sustain the Government in these cases would start the courts down a long and hazardous road that I am not willing to travel--at least without Congressional guidance and direction.*** That the Government mistakenly chose to proceed by injunction does not mean that it could not successfully proceed in another way."

In my opinion, prevention of disclosure in order to avoid serious damage to the intelligence collection effort better serves the national interest than punishment after disclosure. There is a need for specific statutes for injunctive relief.

One can conclude from past practices that there is a general feeling that present statutes are not sufficiently precise to assure success in many cases where court action under authority of existing penal provisions must be called into use in order to protect intelligence sources and methods against unauthorized disclosure.

As an example, the Director of CIA on 22 July 1974 in a

statement to a House Committee hearing on H. R. 15845 (proposed legislation clarifying the mission of CIA) stated:

> "Section (3) of the bill reenforces the charge in the original Act that the Director of Central Intelligence shall be responsible for "protecting intelligence sources and methods from unauthorized disclosure."
>
> * * * *
>
> "Mr. Chairman, I fully agree with this clarification of the precise nature of the charge on the Director to protect intelligence sources and methods against unauthorized disclosure. As you know, I am of the personal opinion that additional legislation is required on this subject to improve our ability to protect intelligence sources and methods against unauthorized disclosure. The contract theory on which the previously mentioned litigation is based is indeed a very slender reed upon which to rely in all cases."

A recommendation to Congress for stronger criminal provisions in the area of Espionage statutes was made by the Commission on Government Security established by the 84th Congress. In June 1957 this commission recommended that Congress enact legislation in the following area to strengthen the Government's hand where unauthorized publication of classified material occurs by persons quite removed from Government service:

> "The Commission recommends that Congress enact legislation making it a crime for any person willfully to disclose without proper authorization, for any purpose whatever, information classified 'secret' or 'top secret', knowing, or having reasonable grounds to believe, such information to have been so classified."

Senator Cotton and Senator Stennis introduced a bill to meet this recommendation. The bill was never brought to a

hearing. Even in the late 1950's when the attitude in this area was far more favorable, efforts to obtain such legislation found little support. The legislative history of the relatively new "Freedom of Information Act" gives little encouragement for enactment of new and stronger legislation covering security violations.

The 89th Congress established the National Commission on Reform of Federal Criminal Law. This Commission has been working with a staff of 50 people for more than three years in drafting revisions to the entire Federal Criminal Code. The 336 page Administration bill known as S 1400 and the McClelland bill of 538 pages known as S-1 have taken into consideration modification and clarification of the Espionage Statutes.

The pending legislation S-1 could be a step in the direction of providing some legislative authority supporting an injunction against publication. S 1400 contains adequate language on this subject but viewed from past legislative history this may not be acceptable to First Amendment sensitive Congress. In the words of Justice Stewart:

> "It is elementary that the successful conduct of international diplomacy and the maintenance of an effective national defense require both confidentiality and secrecy. Other nations can hardly deal with this nation in an atmosphere of mutual trust unless they can be assured that their confidences will be kept."

I. Background

The purpose of this brief is to review the existing affirmative statutory authorities as well as the limiting extent of statutory authorities in connection with the official powers to prevent or punish for public disclosure of national defense classified information. Certain limiting constitutional principles will be discussed.

The Supreme Court case of New York Times Co. v. United States better known as the Pentagon Papers litigation, and the case of United States v. Marchetti have focused on the need for a review of existing authority and the needs for further legislation for protecting classified information.

Certainly an effort to construe the espionage statutes along the line of the meaning that approximates what Congress thought it was doing and what proponents of broader legislation have repeatedly insisted it has done, leaves a great gray zone as to criminal authority in preventing security leaks.

In this connection the fact that there have been few prosecutions premised on publication brought under the espionage laws, even though numerous opportunities have been presented is significant. The prosecution of

Daniel Ellsberg and Anthony Russo for retention of defense information under 18 USC 793(e) was the first effort to apply the espionage statutes to conduct preparatory to publication.

The proceedings in the Pentagon Papers case were completed in a very short time frame leaving little time for review of existing authority and legal precedents in the area of security control. It is generally agreed that the Supreme Court decided the case without making much concrete law. The narrow decision in which the majority of the Court agreed, concluded that on the record the Government had not met its heavy burden to justify injunctive relief against publication. There were nine separate opinions in this case.

The six majority Justices seemed to express a position of reluctance to act in this matter without guidance from Congress. The Government argued the case without regard to legislation. The Government's case was based on the President's constitutional powers as Commander-in-Chief and emphasized his foreign relations authority entitling him to injunctive relief to prevent "grave and irreparable danger" to the public interest.

The Government's brief did not cite the espionage statutes. Neither did the brief state a position whether the New York Times had violated criminal laws by publishing the Pentagon Papers or by their conduct in obtaining and retaining the alleged defense information. All the Justices who concurred in the Judgment stressed the Government's failure to premise its case on legislative authority. One of the Justices stated:

> "Either the Government has the power under statutory grant to use traditional criminal law to protect the country, or if there is not a basis for arguing that Congress has made the activity a crime, it is plain that Congress has specifically refused to grant the authority the Government seeks from this Court. In either case this Court does not have authority to grant this requested relief. It is not for this Court to fling itself into every breach perceived by some Government official nor is it for this Court to take on itself the burden to enacting law, especially a law the Congress has refused to pass."

The Government fared somewhat better in the case of the United States v. Marchetti in the Court of Appeals, Fourth Circuit. This was an action by the U.S. against a former employee for publishing a proposed work in violation of a secrecy agreement and secrecy oath. A preliminary injunction was granted in the District Court and the former employee appealed. The appellant court approved the injunction subject to review of the information under standards laid by the court. The opinion of Chief Judge Haynsworth of the Circuit Court provided in part:

"As we have said, however, Marchetti by accepting employment with the CIA and by signing a secrecy agreement did not surrender his First Amendment right of free speech. The agreement is enforceable only because it is not a violation of those rights. We would decline enforcement of the secrecy oath signed when he left the employment of the CIA to the extent that it purports to prevent disclosure of unclassified information, for, to that extent, the oath would be in contravention of his First Amendment rights.

Thus, Marchetti retains the right to speak and write about the CIA and its operations, and to criticize it as any other citizen may, but he may not disclose classified information obtained by him during the course of his employment which is not already in the public domain."

* * * *

"The Constitution in Article II Part 2 confers broad powers upon the President in the conduct of relations with foreign states and in the conduct of the national defense. The CIA is one of the executive agencies whose activities are closely related to the conduct of foreign affairs and to the national defense. Its operations, generally, are an executive function beyond the control of the judicial power. If in the conduct of its operations the need for secrecy requires a system of classification of documents and information, the process of classification is part of the executive function beyond the scope of judicial review."

* * * *

> "There is a practical reason for avoidance of judicial review of secrecy classifications. The significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context. The courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area."

* * * *

> "Information, though classified, may have been publicly disclosed. If it has been, Marchetti should have as much right as anyone else to republish it. Rumor and speculation are not the equivalent of prior disclosure, however, and the presence of that kind of surmise should be no reason for avoidance of restraints upon confirmation from one in a position to know officially."

* * * *

The Supreme Court refused Mr. Marchetti's further appeal by denying his petition for certiorari. The Court action is recognition of the CIA secrecy agreement. This is in effect enforcement of a contract. It is thus not a criminal action but a civil remedy. Should, however, the court order based on the terms of the contract be violated, Mr. Marchetti could be cited for contempt of court which could result in penal action.

II. Authority for Classifying Material

Article II of the Constitution, provides in Section 1: "The executive power shall be vested in the President of the United Sates of America." In Section 2; it states "The Presiden shall be the Commander-in-Chief of the Army and Navy of the Unit States and in Section 3: "...he shall take care that the laws be faithfully executed." Thus, these provisions of the Constitution set forth the executive power establishing the legal authority for the classification program. The authority is expounded in Executive Order 11652, 37 Fed. Reg. 5209, of June 1, 1972, and its predecessor-Executive Order 10501 of November 9, 1953, 18 Fed. Reg. 7049 which contains the provisions under which the existing system of classification rests.

There is implied legislative recognition of the classification system. Title 18 U.S.C. 798 makes disclosure of certain kinds of "classified information" a crime. Also the Internal Security Act of 1950 (64 Stat. 987, 50 U.S.C. 781) contains legislative recognition of the inherent executive authority to classify sensitive information. Provisions of the Atomic Energy Act of 1954 (68 Stat. 921, 42 U.S.C. 2011 et. seq.) contain further direct legislative foundation for the existing classification system. The Supreme Court in EPA v. Min

410 U.S. 73 (1973), recently decided, at 82, that the first exception to the Freedom of Information Act (5 U.S.C. 552(b)(1) - matters "specifically required by Executive Order to be kept secret in the interest of national defense or foreign policy") expressed a clear congressional intention to preserve the secrecy of classified information per se and, in fact, to even preclude judicial review of the classification process. It is noted that in Dubin v. United States, 363 F. 2d 938 (1966) the Court of Claims, at 942, implicitly held that classification was enough per se to bring equipment under the terms of 18 U.S.C. 793(d).

III. Important elements to be considered in Espionage Statutes.

The major questions concerning the espionage statutes are:

(1) What type of revelation or communication is a necessary element of the particular offense. It is accomplished, in the statutory sense, by publication or preparatory communications;

(2) What state of mind with respect to the consequences for United States' interests is made a

material element of the different offenses, and how should the mental state of a person who publishes information be characterized under the various culpability standards; and,

(3) What information is subjected to statutory restraints under various standards ranging from "information related to the national defense" to "classified communications intelligence?"

IV. (a) The Espionage Statutes.

The relevant espionage statutes are codified in sections 793 to 798 of Title 18 of the United States Code. The basic provisions are sections 793 and 794.

Section 794 contains comprehensive provisions bearing on transfer of defense information to foreigners. Subsection 794(a) punishes actual or attempted communication to a foreign agent of any document or information "relating to the national defense," if the communication is "with intent or reason to believe that it (the information) is to be used to the injury of the United States or to the advantage of a foreign nation."

Subsection 794(b), which is applicable only in time of war, also deals with transfer of information to

foreigners and prohibits collecting, recording, publishing or communicating information about troop movements and military plans "with intent that the same shall be communicated to the enemy."

Subsections 794(a) and 794(b) thus create offenses involving the international transmission of information to foreigners.

Both subsections also criminalize preparatory conduct intended to achieve the proscribed results; subsection 794(a) expressly prohibits attempts, and subsection 794(c) accomplishes much the same results, as it prohibits collecting and recording the protected information with intent to communicate it to the enemy. Subsection 794(d) makes criminal, and punishes equivalently with the completed offense, conspiracies to violate the other subsections.

Provision most applicable to "Leak" cases.

Section 793 of Title 18 U.S.C. (Criminal Code) has primary application to the so-called "leak" problem. Section 793 defines six offenses, each involving conduct which would be preliminary to foreigners' acquisition of information.

Section 793 raises substantial issues as to whether much of the flow of defense information between executive branch employees and the press constitutes serious criminal offenses. The overriding question of interpretation is whether newspapers, their reporters, their informants, or anyone who investigates, accumulates, informs about, or retains defense information as a prelude to public speech is covered by the section. Since section 793 crimes are not defined in terms of the actor's intent to transfer information to foreigners, neither the communication/publication distinction found in 794(a), nor 794(b)'s requirement of an intent to communicate to the enemy directly protect such persons from liability under 793.

Neither 793(a) nor 793(b) could properly be applied to the act of publication because they do not prohibit communications of any kind. Both subsections, however, cover activities which will in many instances occur prior to publication of defense information. Although 793(b) would not be violated if newsmen received oral reports concerning classified information, it nevertheless potentially casts a broad threat of criminal

liability across any publication of a defense-related document or any published analysis based on documentary evidence in the hands of the writer. Although 793(a)'s coverage is not limited to documentary information, it is restricted to entering or obtaining information while upon places connected with the national defense.

No matter how evil the actor's intent, subsections 793(a) and (b) make activity criminal only if the information involved or sought respects the "national defense." The principal problem in construing this term is to find its limits in an area when every facet of civilian life may have an important bearing on the nation's military capabilities.

Section 793 prohibits four basic categories of activities that augment the probability that defense information will come into foreign hands. Subsections 793(a) and 793(b) cover, respectively, obtaining information by physical intrusion into military installations, and copying or otherwise obtaining any document, model, or one of anything connected with the "national defense." Each subsection includes a rather complicated mental requirement, similar to that found in section 794(a);

to be criminal, the conduct must be done "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or the advantage of any foreign nation."

Sections 793(a) and (b) define offenses of acquisitive conduct, not communication of any sort. Nonetheless, except in the oddest sort of situation, to satisfy the statutes' culpability formulations the conduct must be done with the intention to reveal subsequently the information to someone else. If the actor intends only to use the information to contemplate America's defense posture, he does not run afoul of these two laws. Mere satisfaction of individual curiosity could not possibly injure or advantage a nation. In most instances, however, people who make efforts to obtain defense-related information, whether journalists or spies, do so because they envision the possibility of communicating it to others. When the actor expects to tell others, the statute purports to make the acquisition, criminal-depending upon whether the intended or predictable consequences of revelation are that the information

will be used to injure the United States or to advantage any foreign nation.

The Espionage Act - 18 U.S.C. 793(b). (c), (d), and (e)

Title 18 U.S.C. 793(d) states:

> Whoever, lawfully having possesstion of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photographs, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or . . .
>
> * * * *
>
> Shall be fined not more than $10,000 or imprisoned not more than ten years, or both. (Emphasis added)

Subsections (c), (d), and (e) are sweeping statutory authorities and make criminal receipts of material knowing that it has been obtained in violation of other espionage provisions, communication of defense-related material or information to any person not entitled to receive it, and retention of such information.

ubsections 793(d) and 793(e) proscribe willful conduct, hile subsection (c) appears to prohibit any receipt of efense information by one who knows of an actual or ontemplated breach of the espionage laws. Because these statutes do not explicitly on their face require an ulterior intent to harm the United States, subsections (c), (d), and (e)may make criminal nearly all acquisitions by newspapers of "national defense" information, a term defined so broadly by the courts that it comprehends most properly classified information.

Title 18 U.S.C. 793 (d), (e), each create two offenses, one involves willful communication of Defense information to those not entitled to receive it; the other, retention of the material. The claim has been pressed that the statutory terms "communicate, deliver or transmit" do not comprehend publication. The argument is that the draftsmen of the statute perceived a difference between communication and publication and that they intended to make newspaper revelations criminal only when the statutes say "publish." These questions go to the heart of the suggestion of Justice White in the New York Times case, whether newspapers may be criminally punished under 793(e) for obtaining and printing national defense secrets. If publishing is not covered by the statutes, can preliminary and incidental communications and revelations conducted by persons necessary to accomplish publication be held a violation of this statute. Justice White noted that neither publication nor communication

was required to violate the statute; mere retention would suffice. (403 US 713)

(b) Cases in Support of Espionage Statutes

In support of the importance of the use of 18 U.S.C. 793(c), (d), and (e) in security leak incidents, precedents provided in the following court cases are significant in connection with interpretation of previously questioned provisions of this statute, such as the meaning of "national defense" and the questioning of "vagueness" of the statute.

In 1941 the Supreme Court in Gorin v. United States, 312 U.S. 19, upheld a conviction under an earlier version of the Espionage Act which used the terms "connected with" or "relating to" the "national defense." In this case the two terms were challenged as being unconstitutionally vague. However, the court held:

> Finally, we are of the view that the use of the words "national defense" has given them, as here employed, a well understood connotation. They were used in the Defense Secrets Act of March 3, 1911. The traditional concept of war as a struggle between nations is not changed by the intensity of support given to the armed forces by civilians or the extension of the combat area. National defense, the Government maintains, "is a generic concept of broad connotations, referring to the military and naval establishments and the related activities or national preparedness." We agree that the words "national defense" in the Espionage Act carry that meaning . . . . The language employed appears sufficiently definite to apprise the public of prohibited activities and is consonant with due process.

As well, the court approved the following excerpts from the trial court's instructions to the jury on the meaning of the term national defense:

> "The information, document or note might also relate to the possession of such information by another nation and such might also come within the possible scope of this statute. ... Far from the standpoint of military or naval strategy it might not only be dangerous to us for a foreign power to know our weaknesses and our limitations, but it might also be dangerous to us when such a foreign power knows that we know that they know our limitations.
>
> You are, then, to remember that the information, documents or notes, which are alleged to have been connected with the national defense, may relate or pertain to the usefullness, efficiency or availability of any of the above places, instrumentalities or things for the defense of the United States of America. The connection must not be a strained one nor an arbitrary one. The relationship must be reasonable and direct."

Gorin was a citizen of the Soviet Union who acted as its agent in gathering information. He obtained information from a civilian investigator of the Naval Intelligence of the Navy, relating to Japanese activities in the United States. The Court left to the jury the determination of the terms, "connecte with" or "relating to" national defense. The espionage statutes are based on protection of "national defense related" material. Although a broad interpretation was given to the term "national defense," the case also indicated that it would not be criminal to transmit information that the military had made public. Matters often are pieced together from information necessarily given for budget matters and other good reasons leaving some

to argue that it was released to the public domain. This in turn leads to the other extreme that could be drawn from the case of U.S. v Heine. Here the question was whether information culled from periodicals and observations could be termed, "related to the national defense." The Court in this case held that such activities were not covered by the statute. It has been suggested by some legal commentators that the relating to the "national defense" standard passed the vagueness test in Gorin only because the crime involved required the specific intent of injuring the United States or advantaging a foreign nation. "The Espionage Statutes and Publications of Defense Information," 73 Col. L. R. 929 (1973) at 1043. However, it should be noted that the Gorin decision is not explicit in conditioning the statute's validity upon specific intent, and seems to hold that the term "national defense" is constitutionally valid alone and that the specific intent requirement only strengthens its validity. Gorin, supra, at 27, 28.

The test for determining whether a penal statute is too vague is whether it "conveys sufficiently definite warning as to the proscribed conduct when measured by common understanding and practices." Jordan v. DeGeorge,

341 U.S. 223, 231-232. The question is whether well-defined standards have been "developed and accepted in actual practice" to give sufficient notice to those subject to the statutory prohibition that the conduct involved is prohibited. Small Company v. American Sugar Refining Company, 267 U.S. 233, 241; see Hygrade Provision Co. v. Sherman, 266 U.S. 497, 502; Boyce Motor Lines v. United States, 342 U.S. 337, 340-341; United States v. Petrillo, 332 U.S. 1, 8. "Void for vagueness simply means that criminal responsibility should not attach where one could not reasonably understand that his contemplated conduct is proscribed" (United States v. National Dairy Corp., 372 U.S. 29 (1963) at 32-33).

It is submitted that 793(d) has already passed the above tests in the Gorin decision for the reasons that decision sets out concerning the meaning of "relating to national defense."

V. Other Important Provisions of Title 18

Other provisions of Title 18 directed at breaches of security are section 798, which prohibits publication of information dealing with the special category of communications intelligence, and section 795, which

prohibits photographing or making a graphical representation of any vital military equipment or installation that the President has defined as requiring protection against the general dissemination of information relative thereto, without first obtaining permission from the appropriate military authority. Section 797 prohibits subsequent publication of such a photograph.

VI. Miscellaneous Applicable Punitive Statutory Provisions

Atomic Energy Act (68 Stat. 921, as amended, 42 U.S.C. 2274 et seq.)

Section 10 of the Atomic Energy Act (42 U.S.C. 2274-2281) is devoted to the control of information containing "Restricted Data." To the extent, therefore, that information generated by the Department of Defense contains "Restricted Data", these statutory provisions of the Atomic Energy Act are applicable to the information security program of the Department of Defense.

Unlike the ordinary military classification system, the "Restricted Data" classification system has been mandated by Congress. In 42 U.S.C. 2014(y) a provision of the Atomic Energy Act Congress defined "Restricted Data" as follows:

"(y) The term "Restricted Data" means all data concerning: (1) design, manufacture, utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title." Furthermore, the Atomic Energy Act also limits access to "restricted data" of certain specific categories of personnel in 42 U.S.C. 2163 and 42 U.S.C. 2165(b). As well, 42 U.S.C. 2162(g) and 2201(i) and (b) grant the Atomic Energy Commission authority to classify data as "restricted data." Significantly 42 U.S.C. 2274, 2275, 2276 make it a serious crime (with penalties, at one time, up to death) to communicate, receive or tamper with "restricted data" with the specific intent to injure the United States or advantage a foreign nation. It is noted that this section does not require specific intent to constitute the crime. Additionally, 42 U.S.C. 2271(a) expresses a congressional intention to safeguard "restricted data."

There are several aspects of the Act of particular interest. First, the statute has made it a crime knowingly

to communicate information involving restriced data to a person not authorized to receive it. The heaviest penalty is imposed where the communication was made with the intent to injure the United States or to secure an advantage for a foreign power, whereas a lesser penalty is invoked if the communication is made only with "reason to believe" that such will be the result. A still lighter penalty is applicable where the communication was simply not inadvertent, i.e., the communicator knew or had reason to believe that the informant was not authorized to receive it.

Thus it appears that Congress did not wish to limit application of punitive sanctions to situations in which the disclosure was made with an unpatriotic motive, but also wanted punishment for unauthorized disclosures made with belief that the effect would be undesirable or with simple disregard for likely or possible consequences. The "leak" situation, of course, generally involves the last state of mind, for the "leak" is almost never made with an intent to injure the United States or to gain an advantage for a foreign nation; on the contrary, it is more often disclosed for what the source believes to be a patriotic purpose. Specific

recognition by Congress in the Atomic Energy Act of the necessity to punish unauthorized disclosures of Restricted Data made for a variety of motives, therefore, suggests that Congress may also have an appreciation of the need to punish unauthorized disclosures of other defense information "leaked" for a variety of motives.

Similarly, receipt of "Restricted Data" without authority is an offense under the Act, permitting a more severe penalty in the case of receipt with treasonable intent than when only the accused's knowledge of the restricted nature of the data received is proven without respect to his intention in receiving it.

Secondly, the provisions of the Act designed to protect information containing Restricted Data are applicable not only to persons having an existing relationship with the Government, such as employees of the Government, members of the Armed Forces, contractors or licensees of the Atomic Energy Commission, or employees of contractors or licensees, but also to those who previously had a relationship of this kind. There is no similar provision having application to other kinds of defense information not containing Restricted Data. Since,

however, 18 U.S.C. 793 has application to anyone with unauthorized as well as authorized possession of defense information, it too can be applied to persons having a previous employment relationship with the Government or one of its contractors. Nevertheless, it may be desirable to emphasize the apparent intended scope of the Espionage Laws by specifying their general application to persons having had such a previous employment relationship.

A unique and potentially valuable instrument available to protect defense information containing Restricted Data is the injunction section of the Atomic Energy Act, by which a temporary or permanent injunction or restraining order can be obtained from a court to prevent an unauthorized disclosure from being made. There is no comparable provision available to protect other defense information when the disclosure is anticipated or even threatened. Obviously it is more desirable to prevent an unauthorized disclosure of classified information than it is to punish it. Although it is conceivable that such a statute could be used for purposes of censorship, the independence of the judiciary is a safeguard which should be sufficient to overcome any reluctance to provide

statutory authority to enjoin threatened "leaks" of classified information. Nevertheless, many of the same problems arising in a criminal prosecution are also likely to impede the injunction remedy, since the respondent is entitled (Federal Rules of Civil Procedure, 65) to a full hearing on both the facts and the law (though granting a jury trial is a discretionary matter for the determination of the trial court).

Therefore, it can be said that the Atomic Energy Act has made it less difficult to bring a prosecution for the unauthorized disclosure of defense information containing Restricted Data or to prevent its disclosure by injunction. However, the dearth of prosecutions under this Act suggests that there are other primary factors that discourage prosecution.

2. Embezzlement and Theft--Public Money, Property, or Records (18U.S.C. 641).

For a particular fact situation, the general larceny provision of the Criminal Code can be invoked as a basis for criminal prosecution of a "leak." It is applicable only where a record or thing of value is actually

transmitted physically without authority. Such a case may be brought where, for example, a news-media representative has received a record or document with the intent to convert it to his own professional use, knowing that the document or record was converted from its official to an unauthorized use as a source of public information. The news-media representative would be charged with the receipt of converted property, whereas the individual who provided the document without proper authority would be charged with the criminal conversion. The penalty for a "leak" coming within the prohibition of the section, however, would probably be limited to that for a misdemeanor, since the value of the record or document would be measured solely by its physical worth, and not by the value of its contents. (Clark and Marshall, Crimes, 12.01.) This physical value would not amount to more than a few cents in most cases.

The obvious attraction of bringing an indictment under 18 U.S.C. 641, when possible, is the opportunity to avoid the question of treasonable intent, and to permit concentration on proof of the more familiar criminal elements of embezzlement, illegal conversion, or the receipt of stolen property.

3. Concealment, Removal, or Mutilation of Records and Reports (18 U.S.C. 2071)

Another provision is applicable when a physical document or record of the Government has been removed, mutilated, or concealed while perpetrating a "leak," whether custody was obtained legally or illegally. Conviction carries with it a possible three-year imprisonment and a $2,000 fine. Receipt of such a document or record is not punishable in itself, although criminal concealment would generally follow receipt of a "leaked" document or record.

The attraction of this section is the need to prove as essential criminal intent only the intent to conceal, remove, multilate, obliterate, or destroy a Government document, record (etc.).

4. Immunity for Supplying Self-Incriminating Evidence (18 U.S.C. 3486(c).

By granting immunity from criminal prosecution under the authority of 18 U.S.C. 3486(c), the Government would not be faced with a valid refusal to testify on the ground of self-incrimination, for the Supreme Court found specifically in Ullman v. United States, 350 U.S. 422 (1956), that 18 U.S.C. 3486(c) was broad enough to

displace the Fifth Amendment guarantee against self-incrimination. This would entail the convening of a federal grand jury. It is not unlikely, however, that many newspaper reporters would accept the penalty for contempt rather than divulge a confidential source. Thus it is possible that employment of the Immunity Act would only create martyrs among newspaper reporters and not contribute to the solution of the "leak" problem.

5. Conspiracy to Commit an Offense (18 U.S.C. 371).

In addition to the specific conspiracies punishable under the Espionage Laws (see, for example, subsection of 18 U.S.C. 793), the general criminal conspiracy section of the Code has application where the conspiracy is to violate the Atomic Energy Act, the embezzlement and conversion section of the Federal Criminal Code (18 U.S.C. 641), or the protection of official records section of the Code (18 U.S.C. 2071). If, for instance, the author of published material containing "leaked" information entered into an agreement with a Government employee or member of the armed forces, by which agreement the author received validly classified defense information without

official authorization, then he and the supplier of the information are both subject to prosecution for conspiracy under section 371 in addition to possible prosecution for commission of the unlawful act itself. Even if no such defense information was actually provided or printed, the prospective author might still be prosecuted for conspiracy alone, assuming that one of the parties to the agreement did something overt with the purpose of effecting the common criminal design. The essence of the conspiracy is the agreement to violate one of the applicable provisions of the Criminal Code, and an overt act, which need not be criminal itself, done with the purpose of accomplishing that agreement is also essential. Thus, prosecution for conspiracy may be less difficult under some "leak" situations than prosecution for violation of the substantive offense, since elements of the latter need not be proven to establish the former.

On the other hand, proving a criminal conspiracy necessitates the satisfaction of other requirements that may be more difficult to fulfill than the elements of the substantive offense. Proof of the agreement, as well as proof of intent to violate a law (even if the offense

is malum prohibitum), is an essential element. Questions of the defense relation of information, the intent or belief of the transmitter, the wilfullness of the transmission, or the authority of the "leak" recipient may all require satisfactory answers before it can be established that the subject of the agreement was a violation of the Criminal Code.

VII. Protection of Defense Information by Other Democratic Nations

A. Great Britain

1. The Official Secrets Act (see Appendix D)

The theory of privilege, i.e., that all official information is the property of the Crown, provides a basis for the British information-security program not recognized in the United States. In this country the people are assumed to have the "right to know" all information developed by their government unless that right is abridged by some overriding consideration, such as security. Therefore, Crown information can be divulged only when expressly authorized, whereas Government information in the United States can be freely disseminated unless subject to specific prohibitions.

With this basic difference in approach, it is not surprising that the Official Secrets Act is far stronger than comparable legislation in the United States.

By shifting the burden of proof to the defendant for elements of some offenses by creating rebuttable evidentiary presumptions, the Official Secrets Act alleviates the practical difficulty in obtaining a conviction. Moreover, under the Official Secrets Act, portions of the trial may be conducted in camera if the Government so requests to protect classified information (2 of the 1911 Act). The intent or belief of the accused is not an issue in such a case. And where the defendant is accused of committing a misdemeanor by receiving official information, he must prove that the communication to him was contrary to his desire, if he is to escape conviction.

Conviction of a felony requires proof that the defendant's purpose was "prejudicial to the safety of interest of the State" and that the information obtained or communicated "is calculated to be or might be or is intended to be directly or indirectly useful to an enemy"

(1(1)(c) of the 1911 Act). The burden of proving the accused's purpose is, however, appreciably lightened by permitting its satisfaction through the proved circumstances of the case, the conduct of the accused, or his known character, rather than by requiring proof of any particular act tending to show such a purpose (1(2) of the 1911 Act).

A provision of the British law, for which there is no counterpart in the United States Criminal Code, subjects companies and corporations to criminal liability which is also imputed to all directors or officers who cannot prove that the criminal act or omission took place without their knowledge (8(5) of the 1920 Act). The effect of a similar provision in the United States on defense contractors and publishing companies or news-media broadcasting corporations might prove revolutionary. It does not, however, seem probable within the due-process guarantees of a fair trial that any statute shifting the burden of proof to the defendant for any element of a criminal offense would be sustained by the Supreme Court. (But see Casey v. United States, 276 U.S. 413 (1928); Opium, Poppy Control Act of 1942, 36 Stat. 1045, 21 U.S.C. 188 et seq. -- burden of proof is

on the defendant to prove that he comes within any of the exemptions from the general restrictions imposed by the Act). However, this does not mean that evidentiary presumptions to aid prosecution cannot be created by statute.

B. Canada

1. The Official Secrets Act (R.S.C. 1952, c. 198)

The Canadian statute is essentially identical with the British Official Secrets Act, except for a special punitive provision (fine not exceeding five hundred dollars, or imprisonment not exceeding twelve months, or both) when available summary prosecution procedures are elected by the Attorney General (15, c. 198). Consequently, the provision discussion of the British Act appears equally appropriate in regard to the Canadian statute.

C. France

The French Penal Code (see Appendix E), in protecting the "external security of the state," makes comprehensive punitive sanctions available against anyone who compromises sensitive national defense information.

Article 78 defines "secrets of the national defense" in terms far broader than any ever accepted by the courts in the United States (see the Gorin case, discussed supra) when determining the legal definition of "information relating to the national defense." In France, national defense secrets include military information of any nature not made public by the government, and any other general information which by its nature ought to be kept secret in the interest of national defense from anyone not entitled to receive it, or even because it might allow the discovery of information pertaining to national defense. It is likely that such a definition, because of its vagueness, would violate due-process requirements of the United States Constitution.

Article 81, which describes the violation of the French Code known as an "act against the external security of the state," is of primary interest. It makes it an offense to gain access to, knowingly retain, or reveal a national defense secret--or an object or document which may lead to the discovery of such a secret--to the general public or to an unauthorized person, except by authority. Moreover,

allowing anyone to inspect, copy, reproduce, destroy or remove any documents or information which may lead to the discovery of a national defense secret is a basis for criminal prosecution of the individual to whom they were entrusted, even though no more than indiscretion, negligence, or non-compliance with regulations can be proved.

In addition to setting forth punishment for acts against the external security of the state, Article 83 specifically provides for the punishment of attempts as though they were completed offenses. And Article 85 may have some application in "leak" situations to news-media representatives in its provision for punishment as accessories or receivers of anyone who conceals or destroys the documents or objects obtained by a felony or misdemeanor. Article 86 specifies that felonies and misdemeanors against the external security of the state are peace-time as well as wartime offenses, and preserves the jurisdiction of the Codes of Military Justice.

ESPIONAGE LAWS

Title 18, United States Code

792. HARBORING OR CONCEALING PERSONS

Whoever harbors or conceals any person who he knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offense under sections 793 or 794 of this title, shall be fined not more than $10,000 or imprisoned not more than ten years, or both. June 25, 1948, c. 645, 62 Stat. 736.

793. GATHERING, TRANSMITTING, OR LOSING DEFENSE INFORMATION

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal, station, building, office research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause

to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer--

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. June 25, 1948, c. 645, S 1, 62 Stat. 736, amended Sept. 23, 1950, c. 1024, S 18, 64 Stat. ___.

794. GATHERING OR DELIVERING DEFENSE INFORMATION TO AID FOREIGN GOVERNMENT

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or part or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be imprisoned not more than twenty years.

(b) Whoever violates subsection (a) in time of war shall be punished by death or by imprisonment for not more than thirty years.

(c) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the armed forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for not more than thirty years.

(d) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. June 25, 1948, c. 645, 62 Stat. 737.

795. PHOTOGRAPHING AND SKETCHING DEFENSE INSTALLATIONS

(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined not more than $1,000 or imprisoned not more than one year, or both. June 25, 1948, c. 645, 62 Stat. 737.

796. USE OF AIRCRAFT FOR PHOTOGRAPHING DEFENSE INSTALLATIONS

Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, shall be fined not more than $1,000 or imprisoned not more than one year, or both. June 25, 1948, c. 645, 62 Stat. 738.

797. PUBLICATION AND SALE OF PHOTOGRAPHS OF DEFENSE INSTALLATIONS

On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than $1,000 or imprisoned not more than one year, or both. June 25, 1948, c. 645, 62 Stat. 738.

798. DISCLOSURE OF CLASSIFIED INFORMATION

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information--

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes--

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section--

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof. Added Oct. 31, 1951, c. 655 S 24(a), 65 Stat. 719.

798. TEMPORARY EXTENSION OF SECTION 794[1]

The provisions of section 794 of this title, as amended and extended by section 1(a) (29) of the Emergency Powers Continuation Act (66 Stat. 333), as further amended by Public Law 12, Eighty-third Congress, in addition to coming into full force and effect in time of war shall remain in full force and effect until six months after the termination of the national emergency proclaimed by the President on December 16, 1950 (proc. 2912, 3 C.F.R., 1950 Supp., p. 71), or such earlier date as may be prescribed by concurrent resolution of the Congress, and acts which would give rise to legal consequences and penalties under section 794 when performed during a state of war shall give rise to the same legal consequences and penalties when they are performed during the period above provided for. Added June 30, 1953, c. 175, S 4, 67 Stat.

[1]So enacted. See first section 798 enacted on Oct 31, 1951 set out above.

799. VIOLATION OF REGULATIONS OF NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Whoever willfully shall violate, attempt to violate, or conspire to violate any regulation or order promulgated by the Administrator of the National Aeronautics and Space

Administration for the protection or security of any laboratory, station, base or other facility, or part thereof, or any aircraft, missile, spacecraft, or similar vehicle, or part thereof, or other property or equipment in the custody of the Administration or any subcontractor of any such contractor, shall be fined not more than $5,000, or imprisoned not more than one year, or both. Added Pub. L. 85-568, Title III, S 304(c) (1), July 29, 1958, 72 Stat. 434.

ATOMIC ENERGY ACT

Title 42, United States Code

2271. GENERAL PROVISIONS

(a) To protect against the unlawful dissemination of Restricted Data and to safeguard facilities, equipment, materials, and other property of the Commission, the President shall have authority to utilize the services of any Government agency to the extent he may deem necessary or desirable.

(b) No action shall be brought against any individual or person for any violation under this chapter unless and until the Attorney General of the United States has advised the Commission with respect to such action and no such action shall be commenced except by the Attorney General of the Untied States: Provided, however, that no action shall be brought under sections 2272-2275 or 2276 of this title except by the express direction of the Attorney General. Aug. 1, 1946, c. 724, S 221, as added Aug 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 958.

2272. VIOLATION OF SPECIFIC SECTIONS

Whoever willfully violates, attempts to violate, or conspires to violate, any provision of section 2077, 2122, or 2131 of this title, or whoever unlawfully interferes, attempts to interfere, or conspires to interfere with any recapture or entry under section 2138 of this title, shall, upon conviction thereof, be punished by a fine of not more than five years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation shall, upon conviction thereof, be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more

than $20,000 or by imprisonment for not more than twenty years, or both. Aug. 1, 1946, c. 724, S 222, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 958.

2273. VIOLATION OF SECTIONS GENERALLY

Whoever willfully violates, attempts to violate, or conspires to violate, any provision of this chapter for which no penalty is specifically provided or of any regulation or order prescribed or issued under section 2095 or 2201(b), (i), or (p) of this title shall, upon conviction thereof, be punished by a fine of not more than $5,000 or by imprisonment for not more than two years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation, shall, upon conviction thereof, be punished by a fine of not more than $20,000 or by imprisonment for not more than twenty years, or both. Aug 1, 1946, c. 724, S 223, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 958.

2274. COMMUNICATION OF RESTRICTED DATA

Whoever, lawfully or unlawfully, having possession of, access to, control over, or being entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data--

(a) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with intent to injure the United States or with intent to secure an advantage to any foreign nation, upon conviction thereof, shall be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more than $20,000 or imprisonment for not more than twenty years, or both;

(b) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation, shall, upon conviction, be punished by a fine of not more than $10,000 or imprisonment for not more than ten years, or both. Aug 1, 1946, c. 724, S 224, as added Aug 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 958.

2275. RECEIPT OF RESTRICTED DATA

Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, acquires, or attempts or conspires to acquire any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data shall, upon conviction thereof, be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more than $20,000 or imprisonment for not more than twenty years, or both. Aug. 1, 1946, c. 724, S 225, as added Aug 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 959.

2276. TAMPERING WITH RESTRICTED DATA

Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, removes, conceals, tampers with, alters, mutilates, or destroys any document, writing, sketch, photograph, plan, model, instrument, appliance, or note involving or incorporating Restricted Data and used by any individual or person in connection with the production of special nuclear material, or research or development relating to atomic energy, conducted by the United States, or financed in whole or in part by Federal funds, or conducted with the aid of special nuclear material, shall be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury),

or by a fine of not more than $20,000 or imprisonment for not more than twenty years, or both. Aug. 1, 1946, c. 724, S 226, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073 S 1, 68 Stat. 959.

2277. DISCLOSURE OF RESTRICTED DATA

Whoever, being or having been an employee or member of the Commission, a member of the Armed Forces, an employee of any agency of the United States, or being or having been a contractor of the Commission or of an agency of the United States, or being or having been an employee of a contractor of the Commission or of an agency of the United States, or being or having been a licensee of the Commission, or being or having been an employee of a licensee of the Commission, knowingly communicates, or whoever conspires to communicate or to receive, any Restricted Data, knowing or having reason to believe that such data is Restricted Data, to any person not authorized to receive Restricted Data pursuant to the provisions of this chapter or under rule or regulation of the Commission issued pursuant thereto, knowing or having reason to believe such person is not so authorized to receive Restricted Data shall, upon conviction thereof, be punishable by a fine of not more than $2,500. Aug. 1, 1946, c. 724, S 227, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 959.

2278. STATUTE OF LIMITATIONS

Except for a capital offense, no individual or person shall be prosecuted, tried, or punished for any offense prescribed or defined in sections 2274-2276 of this title unless the indictment is found or the information is instituted within ten years next after such offense shall have been committed. Aug. 1, 1946, c. 724, S 228, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 959.

2278a. TRESPASS UPON COMMISSION INSTALLATIONS; ISSUANCE AND POSTING OF REGULATIONS; PENALTIES OR VIOLATION

(a) The Commission is authorized to issue regulations relating to the entry upon or carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of the Commission. Every such regulation of the Commission shall be posted conspicuously at the location involved.

(b) Whoever shall willfully violate any regulation of the Commission issued pursuant to subsection (a) of this section shall, upon conviction thereof, be punishable by a fine of not more than $1,000.

(c) Whoever shall willfully violate any regulation of the Commission issued pursuant to subsection (a) of this section with respect to any installation or other structural barrier shall be guilty of a misdemeanor and upon conviction thereof shall be punished by a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both. Aug. 1, 1946, c. 724, S 229, as added Aug. 6, 1956, c. 1015, S 6, 70 Stat. 1070.

2278b. PHOTOGRAPHING, ETC. OF COMMISSION INSTALLATIONS; PENALTY

It shall be an offense, punishable by a fine of not more than $1,000 or imprisonment for not more than one year, or both --

(1) to make any photograph, sketch, picture, drawing, map or graphical representation, while present on property subject to the jurisdiction, administration or in the custody of the Commission, of any installations or equipment designated by the President as requiring

protection against the general dissemination of information relative thereto, in the interest of the common defense and security, without first obtaining the permission of the Commission, and promptly submitting the product obtained to the Commission for inspection or such other action as may be deemed necessary; or

(2) to use or permit the use of an aircraft or any contrivance used, or designed for navigation or flight in air, for the purpose of making a photograph, sketch, picture, drawing, map or graphical representation of any installation or equipment designated by the President as provided in the preceding paragraph, unless authorized by the Commission. Aug. 1, 1946, c. 724, S 230, as added Aug. 6, 1956, c. 1015, S 6, 70 Stat. 1070.

2279. APPLICABILITY OF OTHER LAWS

Sections 2274-2278b of this title shall not exclude the applicalbe provisions of any other laws. Aug. 1, 1946, c. 724, S 231, formerly S 229, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 959, renumbered and amended Aug. 6, 1956, c. 1015, SS 6, 7, 70 Stat. 1070.

2280. INJUNCTION PROCEEDINGS

Whenever in the judgment of the Commission any person has engaged or is about to engage in any acts or practices which constitute or will constitute a violation of any provision of this chapter, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with such provision, and upon a showing by the Commission that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary injunction, restraining order, or other order may be granted. Aug. 1, 1946, c. 724, S 232, formerly S 230, as added Aug. 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 959, renumbered Aug. 6, 1956, c. 1015, S 6, 70 Stat. 1070.

2281. CONTEMPT PROCEEDINGS

In case of failure or refusal to obey a subpena served upon any person pursuant to section 2201(c) of this title, the district court for any district in which such person is found or resides or transacts business, upon application by the Attorney General on behalf of the United States, shall have jurisdiction to issue an order requiring such person to appear and give testimony or to appear and produce documents, or both, in accordance with the subpena; and any failure to obey such order of the court may be punished by such court as a contempt thereof. Aug. 1, 1946, c. 724, S 233, formerly S 231, as added Aug 30, 1954, 9:44 a.m., E.D.T., c. 1073, S 1, 68 Stat. 960, renumbered Aug. 6, 1956, c. 1015, S 6, 70 Stat. 1070.

MISCELLANEOUS APPLICABLE STATUTES

Title 18, United States Code

641. PUBLIC MONEY, PROPERTY OR RECORDS

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted --

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater. June 25, 1948, c. 645, 62 Stat. 725.

2071. CONCEALMENT, REMOVAL, OR MUTILATION GENERALLY

(a) Whoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or, with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States, shall be fined not more than $2,000 or imprisoned not more than three years, or both.

(b) Whoever, having the custody of any such record, proceeding, map, book, document, paper, or other thing, willfully and unlawfully conceals, removes, mutilates, obliterates, falsifies, or destroys the same, shall be fined not more than $2,000 or imprisoned not more than three years, or both; and shall forfeit his office and be disqualified from holding any office under the United States. June 25, 1948, c. 645, 62 Stat. 795.

3486. COMPELLED TESTIMONY TENDING TO INCRIMINATE WITNESSES; IMMUNITY

(c) Whenever in the judgment of the United States attorney the testimony of any witness, or the production of books, papers, or other evidence by any witness, in any case or proceeding before any grand jury or court of the United States involving any interference with or endangering of, or any plans or attempts to interfere with or endanger, the national security or defense of the United States by treason, sabotage, espionage, sedition, seditious conspiracy, violations of chapter 115 of title 18 of the United States Code, violations of the Internal Security Act of 1950 (64 Stat. 987), violations of the Atomic Energy Act of 1946 (60 Stat. 755), as amended, violations of sections 212(a) (27), (28), (29) or 241(a) (6), (7) or 313(a) of the Immigration and Nationality Act (66 Stat. 182-186; 204-206; 240-241), and conspiracies involving any of the foregoing, is necessary to the public interest, he, upon the approval of the Attorney General, shall make application to the court that the witness shall be instructed to testify or produce evidence subject to the provisions of this section, and upon order of the court such witness shall not be excused from testifying or from producing books, papers, or other evidence on the ground that the testimony or evidence required of him may tend to incriminate him or subject him to a penalty or forfeiture. But no such witness shall be prosecuted or subjected to any penalty or forfeiture for or on account of any transaction, matter, or thing concerning which he is compelled, after having

claimed his privilege against self-incrimination, to testify or produce evidence, nor shall testimony so compelled be used as evidence in any criminal proceeding (except prosecution described in subsection (d) hereof) against him in any court.

(d) No witness shall be exempt under the provision of this section from prosecution for perjury or contempt committed while giving testimony or producing evidence under compulsion as provided in this section. As amended Aug. 20, 1954, c. 769, S 1, 68 Stat. 745.

371. CONSPIRACY TO COMMIT OFFENSE OR TO DEFRAUD UNITED STATES

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined not more than $10,000 or imprisoned not more than five years, or both.

If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor. June 25, 1948, c. 645, 62 Stat. 701.

HALSBURY'S STATUTES OF ENGLAND
Second Edition, Volume 5

THE OFFICIAL SECRETS ACT, 1911

1. Penalties for spying. -- (1) If any person for any purpose prejudicial to the safety or interests of the State--

(a) approaches (inspects, passes over) or is in the neighborhood of, or enters any prohibited place within the meaning of this Act; or

(b) makes any sketch, plan, model, or note which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy; or

(c) obtains, (collects, records, or publishes,) or communicates to any other person (any secret official code word, or pass word, or) any sketch, plan, model, article, or note, or other document or information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy;

he shall be guilty of felony. . . .

(2) On a prosecution under this section, it shall not be necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State, and, notwithstanding that no such act is proved against him, he may be convicted if, from the circumstances of the case, or his conduct, or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State; and if any sketch, plan, model, article, note, document, or information relating to or used in any prohibited place within the meaning of this Act, or anything in such a place (or any secret official code word or pass word), is made, obtained, (collected, recorded, published), or communicated by any person other than a person acting under lawful authority, it shall be deemed to have been made, obtained, (collected, recorded, published) or communicated for a purpose prejudicial to the safety or interests of the State unless the contrary is proved. (2206)

2. Wrongful communication, etc., of information. -- (1) If any person having in his possession or control (any secret official code word, or pass word, or) any sketch, plan, model, article, note, document, or information which relates to or is used in a prohibited place or anything in such a place, or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by any person holding office under His Majesty or which he has obtained (or to which he has had access) owing to his position as a person who holds or has held office under His Majesty, or as a person who holds or has held a contract made on behalf of His Majesty, or as a person who is or has been employed under a person who holds or has held such an office or contract, --

(a) communicates the (code word, pass word,) sketch, plan, model, article, note, document, or information to any person, other than a person to whom he is authorized to communicate it, or a person to whom it is in the interest of the State his duty to communicate it, or,

(aa) Uses the information in his possession for the benefit of any foreign power or in any other manner prejudicial to the safety or interests of the State;)

(b) retains the sketch, plan, model, article, note, or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it (or fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof) (or,

(c) fails to take reasonable care of, or so conducts himself as to endanger the safety of the sketch, plan, model, article, note, document, secret official code or pass word or information:)

that person shall be guilty of a misdemeanour.

(1A) If any person having in his possession or control any sketch, plan, model, article, note, document, or information which relates to munitions of war, communicates it directly or indirectly to any foreign power, or in any

other manner prejudicial to the safety or interests of the State, that person shall be guilty of a misdemeanour.)

(2) If any person receives any (secret official code word, or pass word, or) sketch, plan, model, article, note, document, or information, knowing, or having reasonable ground to believe, at the time when he receives it, that the (code word, pass word,) sketch, plan, model, article, note, document, or information is communicated to him in contravention of this Act, he shall be guilty of a misdemeanour, unless he proves that the communication to him of the (code word, pass word,) sketch, plan, model, article, note, document, or information was contrary to his desire.

3. Definition of prohibited place.

* * * * *

6. Power to arrest.-- Any person who is found committing an offence under this Act, whether that offence is a felony or not, or who is reasonably suspected of having committed, or having attempted to commit, or being about to commit, such an offence, may be apprehended and detained in the same manner as a person who is found committing a felony. (2210)

* * * * *

8. Restriction on prosecution.-- A prosecution for an offence under this Act shall not be instituted except by or with the consent of the Attorney-General:

Provided that a person charged with such an offence may be arrested, or a warrant for his arrest may be issued and executed, and any such person may be remanded in custody or on bail, notwithstanding that the consent of the Attorney-General to the institution of a prosecution for the offence has not been obtained, but no further or other proceedings shall be taken until that consent has been obtained. (2212)

9. Search warrants.-- (1) If a Justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorizing any constable named therein to enter at any time any premises or place named in the warrant, if necessary, by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note, or document, or anything of a like nature or anything which is evidence of an offence under this Act having been or being about to be committed, which he may find on the premises or place or on any such person, and with regard to or in connection with which he has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.

(2) Where it appears to a superintendent of police that the case is one of great emergency and that in the interests of the State immediate action is necessary, he may by a written order under his hand give to any constable the like authority as may be given by the warrant of a justice under this section. (2213)

* * * * *

12. Interpretation.-- In this Act, unless the context otherwise requires,--

* * * * *

Expressions referring to communicating or receiving include any communicating or receiving, whether in whole or in part, and whether the sketch, plan, model, article, note, document, or information itself or the substance, effect, or description thereof only be communicated or received; expressions referring to obtaining or retaining any sketch, plan, model, article, note, or document, include the copying or causing to be copied the whole or any part of any sketch, plan, model, article, note, or document; and expressions referring to the communication of any sketch, plan, model, article, note or document include the transfer or transmission of the sketch, plan, model, article, note or document;

The expression "document" includes part of a document;

(The expression "munitions of war" includes the whole or any part of any ship, submarine, aircraft, tank or similar engine, arms and ammunition, torpedo, or mine, intended or adapted for use in war, and any other article, material, or device, whether actual or proposed, intended for such use;)

* * * * *

THE OFFICIAL SECRETS ACT, 1920

* * * * *

6.-- (1) Where a chief officer of police is satisfied that there is reasonable ground for suspecting that an offence under section one of the principal Act has been committed and for believing that any person is able to furnish information as to the offence or suspected offence, he may apply to a Secretary of State for permission to exercise the powers conferred by this subsection and, if such permission is granted, he may authorize a superintendent of police, or any police officer not below the rank of inspector, to require the person believed to be able to furnish information to give any information in his power relating to the offence or suspected offence, and, if so required and on tender of his reasonable expenses, to attend at such reasonable time and place as may be specified by the superintendent or other officer; and if a person required in pursuance of such an authorization to give information, or to attend as aforesaid, fails to comply with any such requirement or knowingly gives false information, he shall be guilty of a misdemeanour.

(2) Where a chief officer of police has reasonable grounds to believe that the case is one of great emergency and that in the interest of the State immediate action is necessary, he may exercise the powers conferred by the last foregoing subsection without applying for or being granted the permission of a Secretary of State, but if he does so shall forthwith report the circumstances to the Secretary of State.

(3) References in this section to the chief officer of police shall be construed as including references to any other officer of police expressly authorized by a chief

officer of police to act on his behalf for the purposes of this section when by reason of illness, absence, or other cause he is unable to do so.) (2371)

7. Attempts, incitements, etc.-- Any person who attempts to commit any offence under the principal Act or this Act, or solicits or incites or endeavours to persuade another person to commit an offence, or aids or abets and does any act preparatory to the commission of an offence under the principal Act or this Act, shall be guilty of a felony or a misdemeanour or a summary offence according as the offence in question is a felony, a misdemeanour or a summary offence, and on conviction shall be liable to the same punishment, and to be proceeded against in the same manner, as if he had committed the offence. (2372)

8. Provisions as to trial and punishment of offences.-- (1) Any person who is guilty of a felony under the principal Act or this Act shall be liable to penal servitude for a term of not less than three years and not exceeding fourteen years.

(2) Any person who is guilty of a misdemeanour under the principal Act or this Act shall be liable on conviction on indictment to imprisonment, with or without hard labour, for a term not exceeding two years, or, on conviction under the Summary Jurisdiction Acts, to imprisonment, with or without hard labour, for a term not exceeding three months or to a fine not exceeding fifty pounds, or both such imprisonment and fine:

Provided that no misdemeanour under the principal Act or this Act shall be dealt with summarily except with the consent of the Attorney General.

(3) For the purposes of the trial of a person for an offence under the principal Act or this Act, the offence shall be deemed to have been committed either at the place in which the same actually was committed, or at any place in the United Kingdom in which the offender may be found.

(4) In addition and without prejudice to any powers which a court may possess to order the exclusion of the public from any proceedings if, in the course of proceedings before a court against any person for an offence under the principal Act or this Act or the proceedings on appeal, or in the course of the trial of a person for felony or misdemeanour under the principal Act or this Act, application is made by the prosecution, on the ground that the publication of any evidence to be given or of any statement to be made in the course of the proceedings would be prejudicial to the national safety, that all or any portion of the public shall be excluded during any part of the hearing, the court may make an order to that effect, but the passing of sentence shall in any case take place in public.

(5) Where the person guilty of an offence under the principal Act or this Act is a company or corporation, every director and officer of the company or corporation shall be guilty of the like offence unless he proves that the act or omission constituting the offence took place without his knowledge or consent. (2373)

NOTE:

(1) These are selected sections which appear to be most pertinent to the immediate problem.

THE FRENCH PENAL CODE

Article 78

Within the meaning of this Code, the following are considered secrets of the national defense:

1. Military as well as diplomatic, economic or industrial information, which, by its nature, is not to be made known except to those entitled thereto, and which ought to be kept secret from anybody else in the interest of the national defense;

2. Goods, materials, documents, designs, drafts, maps, surveys, pictures or other reproductions and all other documents whatsoever which, by their nature, are not to be made known except to those who are entitled to use and to have them, and which ought to be kept secret from anybody else because they may allow the discovery of information pertaining to the categories mentioned in the foregoing paragraph;

3. Military information of any nature whatsoever not made public by the government and not included in the above list and the publication, propagation, disclosure or dissemination of which has been prohibited by law or decree of the Council of Ministers;

4. Information pertaining to measures taken for the discovery and arrest of principals and accessories of felonies and misdemeanors against the external security of the state, or to procedure, investigation or pleadings.

Article 81

Any French national or foreigner shall be guilty of an act against the external security of the state and sentenced to punishment in accordance with Article 83, who:

1. For a purpose other than that of revealing it to a foreign power or its agents, either unauthorizedly and by any means whatsoever, gains access to a national defense secret, or knowingly and unauthorizedly retains an object or document classified as a secret of national defense,

or one which may lead to the discovery of such a secret, or reveals such a secret, in any form or manner, to the public or to an unauthorized person;

2. By indiscretion, negligence or non-compliance with regulations, allows to be destroyed, taken away or removed, wholly or in part, even if only temporarily, any goods, materials, documents or information entrusted to him, the knowledge of which might lead to the discovery of a national defense secret, or allows anyone to inspect, to copy or to reproduce it, even if only in part;

3. Without being duly authorized, betrays or supplies to any person acting for a foreign power or firm, either a device concerning the national defense, or information, research or processes dealing with such a device or with an industrial exploitation thereof adapted to the national defense.

Article 83

If committed in time of war, acts against the external security of the state shall be punished by hard labor for a limited time.

If committed in time of peace they shall be punished by jailing from one to five years and by fine from 360,000 to 3,600,000 francs.

Nevertheless, in the case of offenses under Article 79, paragraph 1, Article 80, paragraph 1, Article 81, paragraph 1, Articles 82, 103 or 104, jail sentences may be increased to ten years and the fine to 7,200,000 francs.

In time of war all other knowingly performed acts, differently punishable by other laws, likely to result in harm to the national defense shall be punished by jailing from one to five years and by fine from 360,000 to 3,600,000 francs.

Furthermore, convicts may always be sentenced to loss of civil rights provided by Article 42 of this Code, for no less than five nor more than twenty years. They may also be restricted in their freedom or movement.

The attempt shall be punished like the completed offense.

Article 85

Any French national or foreigner, other than those subject to Articles 60 and 460, shall be punished as accessories or receivers, who:

1. Aware of the interests and purposes of principals of felonies or misdemeanors against the external security of the state, provides them with aid, comfort, lodging, retreat or meeting places;

2. Knowingly carries the messages of principals of felonies or misdemeanors, or in any way knowingly helps them in the search for, or the concealment, carriage or transmission of the object of the felony or misdemeanor;

3. Knowingly conceals objects and implements which were or were to be used for the commission of the felony or misdemeanor and the objects, materials or documents which have been obtained by the felony or misdemeanor.

RECOMMENDATIONS OF THE AD HOC WORKING GROUP ON

UNAUTHORIZED DISCLOSURES

1. Conduct a review of current hard-copy distribution categories to identify those recipients who have a valid need to be informed of current intelligence information in general terms, but who do not have a "must know" need for the type of highly-detailed reportage contained in intelligence publications.

2. Institute the use of a publication similar to the Executive Summary (EXSUM) as a substitute for NIB/DIN distribution to those recipients who do not require such detailed information.

3. Establish new and more restrictive distribution list for high-leak potential intelligence reports. Utilize such lists to further reduce dissemination of "high-risk" items. Also utilize authorized disclosures via special high-level ad hoc groups formed for this purpose.

4. Carefully edit reports with high-leak potential to remove sensitive source data and collection capability indicators. Also, reduce unessential technical details, wherever possible.

5. Encourage high-level policy planners to seek assistance in sanitizing intelligence reports that they consider suitable for release to the press.

6. Establish an indoctrination program for all personnel concerned to acquaint them with:

a. The real threat to sensitive and costly intelligence collection programs posed by unauthorized disclosures.

b. The means of preventing such disclosures.

c. Possible ways to reduce the impact of an anticipated unauthorized disclosure.

d. The personal responsibilities of each individual in this endeavor.

7. Publish security flyers periodically to remind all concerned of the threat posed by unauthorized disclosures. Such flyers should be disseminated to both personnel involved in the production of intelligence reports and to recipients of intelligence information.

8. Institute a system of staggered distribution of high-leak potential items, utilizing EXSUM, ORCON or other highly restrictive security markings, for initial distribution in order to reduce the attractiveness of such items.

9. Consider the usage of special "no copy" paper for highly sensitive items identified/selected for extremely limited local distribution.